National Infrastructure Protection Center CyberNotes

Issue #2000-03 *February 16, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 28 and February 10, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[1]	Spectra 1.0	A security vulnerability exists in the template, invoke.cfm. which may allow remote unauthenticated users to make use of the Remote Access Service.	Patch available at: http://download.allaire.com/patches/ASB00-04.zip	Allaire Spectra Unauthenticated RAS Access	Low	Bug discussed in newsgroups and websites. Exploit has been published.
AVT[2]	Rightfax Web Client v5.2	A vulnerability exists which would allow remote users, once logged in, to hijack sessions of other users by guessing a predictable session ID.	No workaround or patch available at time of publishing.	Rightfax Webclient Predictable Session Number	Medium	Bug discussed in newsgroups and websites.

[1] Securiteam, February 1, 2000.

[2] Securiteam, February 3, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Axis Communications[3]	Axis 700 Network Scan Server 1.12	A vulnerability exists which could allow malicious users to access administrator URLs (or any other directories that need authentication) without having to enter a username and password.	Patch available at: http://www.se.axis.com/techsup/scan_servers/axis_700/index.html	Axis 700 Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Caldera Systems, Inc.[4]	OpenLinux Desktop 2.3	A buffer overflow exists in the mount and umount commands, which are setuid root.	The upgrade packages can be found at: ftp://ftp.calderasystems.com/pub/openlinux/updates/2.3/current/RPMS	Caldera Mount/Umount Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Checkpoint Software[5]	Firewall-1 4.0, 3.0	A vulnerability exists in the way that Checkpoint FireWall-1 handles packets sent from a FTP server to a connecting client. A malicious user may be able to exploit this weakness to establish connections to any machine residing behind a FireWall-1 machine, or send packets to a network protected by a FireWall-1.	No workaround or patch available at time of publishing.	Checkpoint FireWall-1 FTP Server	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Checkpoint Software [6]	Firewall-1 3.0	Firewall-1 includes the ability to alter script tags in HTML pages before passing them to the client's browser. This function can be bypassed by adding an extra opening angle bracket, which could lead to unauthorized scripts bypassing the firewall. This may lead to remote compromise of the client system.	No workaround or patch available at time of publishing.	Checkpoint Firewall-1 Script Tag Checking Bypass	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cobalt[7]	RaQ1, 2, 3	A security vulnerability exists in the User Management CGI that could allow a remote malicious user to change any user's password including that of administrators.	No workaround or patch available at time of publishing.	Cobalt RaQ Password CGI	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Infosec Security Vulnerability Report No: Infosec.20000207.axis700.a, February 7, 2000.
[4] Caldera Systems, Inc. Security Advisory, CSSA-2000-002.0, February 3, 2000.
[5] SecurityFocus, February 9, 2000.
[6] Securiteam, January 30, 2000.
[7] Cobalt Networks Security Advisory, 01.31.2000, January 31, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Daniel Beckham[8]	The Finger Server 0.82beta	Due to insufficient input checking, it is possible for remote unauthenticated users to execute shell commands on the server, which will run with the privileges of the webserver.	No workaround or patch available at time of publishing.	Finger Server Pipe	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Debian[9]	Linux 2.0, 2.0r5, 2.1, 2.2, 2.2pre potato	A vulnerability exists in the master boot record (MBR) installed by default, which could allow a malicious user with local access to bypass any BIOS or LILO boot passwords.	A patch was made available, and published as part of the 2.2.6 Debian boot floppies.	Debian GNU/Linux MBR password bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Debian[10]	Linux 2.1	A vulnerability exists in the apcd package, which could allow a malicious user to create a symlink to another file. This could lead to a compromise of the root account.	Patch available at: (Please replace 'alpha' with the appropriate architecture) http://security.debian.org/dists/stable/updates/binary-alpha/apcd_0.6a.nr-4slink1_alpha.deb	Debian APCD Symlink	**High**	Bug discussed in newsgroups and websites.
Deerfield.com[11]	Serv-U FTP-Server v2.5b	A buffer overflow exists in the Windows Api "SHGetPathFromIDList"	No workaround or patch available at time of publishing.	Serv-U FTP SHGetPathFromIDList	Low	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD/ OpenBSD[12]	FreeBSD 2.8, 3.0, 3.3; OpenBSD 2.4, 2.5, 2.6	A vulnerability exists in the procfs code, which enables local users to obtain root access to the machine.	Patches are available at: OpenBSD: http://www.openbsd.org/errata.html#procfs FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:02/procfs.patch	FreeBSD/ OpenBSD Procfs Security	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
H. Nomura[13]	Tiny FTPDaemon 0.52	A buffer overflow exists which could allow remote malicious users to execute arbitrary code on the server.	No workaround or patch available at time of publishing.	Tiny FTPd Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[8] Bugtraq, February 3, 2000.
[9] SecurityFocus, February 2, 2000.
[10] Debian Security Advisory, February 1, 2000.
[11] USSR Labs, USSR-2000032, February 4, 2000.
[12] FreeBSD Security Advisory: FreeBSD-SA-00:02.procfs, January 28, 2000.
[13] Securiteam, February 3, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Mechfire [14]	WarFTPd 1.67-3, 1.66x4s	Due to improper bounds checking in the code that handles the MKD and CWD commands, it is possible to remotely crash the server.	Version 1.67-4 has been patched against this vulnerability, and is available at: http://war.jgaa.com/alert/files/ward167-4.zip Also, upgrading to version 1.71 will fix this problem. 1.71 is available at: Http://war.jgaa.com/alert/files/ward171-0.zip	War-FTPd CWD/MKD Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft	Windows NT 4.0 SP1-SP6	The LsaQueryInformationPolicy() function can be used to retrieve an NT domain's SID from any workstation in that domain. An anonymous user through a null session can do this remotely. That SID can then be used to obtain lists of user's names and SIDs for brute force attacks.	No workaround or patch available at time of publishing.	NT LsaQueryInformationPolicy() Domain SID Leak	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[15]	FrontPage 98/2000	FrontPage contains two vulnerabilities, which reveal system configuration information. A malicious user can discover the name of the anonymous Internet account and learn physical paths on system	No workaround or patch available at time of publishing. If you don't use the functionality provided by FrontPage, then you should remove, not only shtml.dll and htimage.exe but also all other files associated with FrontPage.	MS FrontPage System Information	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[16] ***Microsoft has re-released the version of this patch that applies to Windows 2000[17]***	**Index Server 2.0;** **Windows 2000 Indexing Service**	**Two security vulnerabilities exist in the Index Server that could allow a malicious user to view (but not to change/add/delete) files on a web server. The second vulnerability could reveal where web directories are physically located on the server.** ***The security bulletin was revised on February 4th and again on February 11th.***	**Patch available at:** **Index Server 2.0:** **Intel:** **http://www.microsoft.com/downloads/release.asp?ReleaseID=17727** **Alpha:** **http://www.microsoft.com/downloads/release.asp?ReleaseID=17728** **Indexing Services for Windows 2000:** **Intel:** **http://www.microsoft.com/downloads/release.asp?ReleaseID=17726** ***More information can be found at:*** http://www.microsoft.com/technet/security/bulletin/ms00-006.asp	**Malformed Hit-Highlighting Argument**	**Medium /Low**	**Bug discussed in newsgroups and websites.** **Exploit has been published.**

[14] Bugtraq, February 1, 2000.
[15] Cerberus Information Security Advisory (CISADV000203), February 3, 2000.
[16] Microsoft Security Bulletin, MS00-006, January 26, 2000.
[17] Microsoft Security Bulletin, MS00-006, February 11, 2000.

Hardware/ Operating System/ Vendor	**Equipment/ Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
Microsoft[18]	Internet Explorer 4/5	A security vulnerability exists in Microsoft's Java Virtual Machine, which allows a Java applet to read files in certain directories. This can be done via the getSystemResourceAsStream() function.	No workaround or patch available at time of publishing. ***This vulnerability is quite dangerous and immediate de-activation of IE's Java functionality provided by Microsoft VM is highly recommended.***	Microsoft Java Virtual Machine GetSystem ResourceAs Stream	**Very High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Microsoft[19]	IIS 5.0, 4.0, 3.0	Active Server Pages (ASP) that have errors in them or in their components can cause error messages to be served to the browser that include path information for files used in the creation of the .asp file. These files can then be downloaded and may include sensitive information such as resource locations, website and network structure, and business models.	Workaround: Thoroughly debug all ASP code before publishing.	NT IIS ASP VBScript Runtime Error Viewable Source	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[20]	Outlook Express 5.0	Microsoft Outlook Express 5, and possibly other e-mail clients that parse HTML messages, can be made to run Active Scripting that will read any new messages that arrive after the hostile code has been run. By sending specially created e-mail message, remote malicious users can retrieve any open e-mail you currently have, gaining sensitive information.	Workaround: Disable active scripting	MS Outlook Express 5 JavaScript E-mail Access Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[18] Bugtraq, February 1, 2000.
[19] SecurityFocus, February 9, 2000.
[20] Bugtraq, February 1, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[21]	Windows NT	A buffer overflow exists in the SHGetPathFromIDList() API. A user can create a malicious shortcut file that will cause any calling application using it to crash. This vulnerability affects many applications, such as FTP servers, that allow the use of shortcuts.	No workaround or patch available at time of publishing.	Microsoft Windows Shortcut	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22]	Windows NT Workstation 4,0; Server 4.0; Server 4.0, Enterprise Edition	A security vulnerability exists which could allow a malicious user to create/delete/modify files in the Recycle Bin of another user who shared the machine.	Patch available at: Intel: http://www.microsoft.com/downloads/release.asp?ReleaseID=17606 Alpha: http://www.microsoft.com/downloads/release.asp?ReleaseID=17607	Microsoft Recycle Bin Creation	Medium	Bug discussed in newsgroups and websites.
Multiple Firewalls[23]	Multiple Firewalls	It is possible to cause certain firewalls to open a TCP port by fooling a protected FTP server into echoing "227 PASV" commands out through the firewall.	No workaround or patch available at time of publishing.	Multiple Firewall FTP Application Level Gateway PASV	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Web Shopping Carts[24]	Web Shopping Carts	The ISS X-Force recently released an advisory stating that an audit of 11 Web shopping cart applications revealed that they're vulnerable to various types of form tampering, which includes changing prices of purchased items and bypassing security restrictions. This is accomplished with false HTTP Referer headers.	The following applications were found vulnerable: Check It Out http://ssl.adgrafix.com @Retail http://www.atretail.com Cart32 2.6 http://www.cart32.com CartIt 3.0 http://www.cartit.com Make-a-Store OrderPage http://www.make-a-store.com SalesCart http://www.salescart.com SmartCart http://www.smartcart.com Shoptron 1.2 http://www.shoptron.com EasyCart http://www.easycart.com Intellivend http://www.intellivend.com WebSiteTool http://www.websitetool.com All vendors of the above list have released patches EXCEPT EasyCart, Intellivend and WebSiteTool. All users should download updates from the URL given.	Web Shopping Carts HTTP Referer Headers	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[21] NTBugtraq, February 7, 2000.
[22] Microsoft Security Bulletin, MS00-07, February 1, 2000.
[23] Bugtraq, February 10, 2000.
[24] ISS E-Security Alert, February 1, 2000.

Hardware/ Operating System/ Vendor	**Equipment/ Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
Novell[25]	Border Manager 3.0, 3.5	A security vulnerability exists which enables malicious users to perform a Denial of Service attack against the firewall, causing it to stop responding.	Workaround: Unload the CSATPRX.NLM or block incoming requests to port 2000 from the external interface.	Novell Border Manager Audit Trail Proxy DoS	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Novell[26]	Groupwise Web Access 5.5 Enhancement Pack	A Denial of Service vulnerability exists when a large character string is sent by a browser and is processed by the servlet gateway. The server will need to be rebooted to restore normal operation.	GroupWise Enhancement Pack 5.5 sp1 has been released which addresses this problem. To obtain it, contact Novell Technical Support.	Novell GroupWise 5.5 Enhancement Pack Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Progress[27]	WebSpeed 3.0	A vulnerability exists in the WSISA Messenger Administration Utility, which is remotely accessible from any web browser. This utility displays sensitive web server statistics and grants capabilities to administer certain functions of the web server, and can be accessed without any authentication requirements.	Patch available at: http://www.progress.com/patches/patchlst/availpatche.html	Progress WebSpeed Administration Utility Configuration	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[28]	Open Server 5.0.5	The default configuration gives local users read/write access to the SNMPd via a default writable community string. This allows local users to gain additional privileges, which could lead to a system compromise.	Information on how to patch the vulnerability can be found at: ftp://ftp.sco.com/SSE/security_bulletins/SB-00.04a	SCO OpenServer SNMPD Default Community	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[29]	Linux 6.3, 6.1	A vulnerability exists in the way the GNU <make> command handles being fed Makefile contents. A malicious user could cause unauthorized command to be execute with the privileges of the user-executing make.	Patches are available at: Intel: ftp://ftp.suse.com/pub/suse/i386 Alpha: ftp://ftp.suse.com/pub/suse/axp/	SuSE Make Root Compromise Vulnerability	**High**	Bug discussed in newsgroups and websites.

[25] SecurityFocus, February 4, 2000.
[26] SecurityFocus, February 7, 2000.
[27] Bugtraq, February 3, 2000.
[28] SCO Security Bulletin, 2000.04, February 8, 2000.
[29] SuSE Security Announcement, February 9, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sybergen[30]	SyGate 3.11, 2.0	A vulnerability exists in the Remote Administration Engine (RAE) which allows access from outside the SyGate gateway. Since the RAE was designed to be accessible only from behind the SyGate gateway there is no user authentication when accessing it.	Patch available at: http://www.sygate.com/SyGate562.exe	SyGate Remote Administration Engine	**High**	Bug discussed in newsgroups and websites.
T.C.X DataKonsult[31]	MySQL 3.22.26-3.22.30, 3.23.8-10	A vulnerability exists in the password verification scheme, which will allow any user on a machine that has been granted access to the database. This access is granted without knowing the account name or password of the user.	No workaround or patch available at time of publishing.	MySQL Unauthenticated Remote Access	Medium	Bug discussed in newsgroups and websites.
True North Software[32]	Internet Anywhere Mail Server 3.1.3	A Denial of Service vulnerability exists by initiating a large amount of connections to port 25.	No workaround or patch available at time of publishing.	Internet Anywhere Mail Server Connection Overload	Low	Bug discussed in newsgroups and websites. Exploit has been published.
True North Software[33]	Internet Anywhere Mail Server 3.1.3	Submitting a RETR command with a message ID argument longer than 10 numeric characters will result in a crash of the Internet Anywhere Mail Server.	No workaround or patch available at time of publishing.	Internet Anywhere Mail Server RETR Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Wired Community Software[34]	WWWThreads 5.0b3 and prior	Security vulnerability exists in wwwthreads and its SQL information retrieval engine which could allow remote malicious users to gain access to usernames and passwords. Additional SQL commands could be inserted into legitimate queries, gaining elevated security access, and leading to possible compromise of the wwwthreads security.	Wired Community Software has released a fixed version of WWWThreads, available at: Demo version: http://www.wwwthreads.com/download.html Licensed version: Http://www.wwwthreads.com/licensed/	WWWThreads SQL Command Input	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[30] Bugtraq, January 28, 2000.
[31] SecurityFocus, February 9, 2000.
[32] SecurityFocus, February 10, 2000.
[33] SecurityFocus, February 10, 2000.
[34] SecurityFocus, February 3, 2000.

Hardware/ Operating System/ Vendor	**Equipment/ Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
Zeus Technologies [35]	Zeus Web Server 3.1x, 3.3x	A vulnerability exists which could allow a malicious user to view the source of CGI scripts.	Zeus Technologies has provided patches for all 14 platforms Zeus Web Server is compatible with which rectifies this issue. They may be downloaded at: ftp://ftp.zeustechnology.com/pub/products/z3	Zeus Web Server Null Terminated Strings	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between January 25, and February 10, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 51 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
February 10, 2000	Twinge.c	Script that crashes almost any Windows box on your local network.	
February 9, 2000	MiM.c	MiM can be used to redirect the flow between two hosts through a third host.	
February 8, 2000	**Amd.tgz**	**Rpc.amd remote exploit that includes a spoofed source address.**	
February 8, 2000	Rawpowr.c	Rawpowr.c can access a block device containing an EXT2 file system in raw mode, changing all executables into suid executables.	

[35] S.A.F.E.R. Security Bulletin 000209.EXP.1.2, February 9, 2000.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
February 8, 2000	**Stachel.tgz**	**StacheldrahtV4 combines features of the 'trinoo' distributed Denial of Service tool, with those of the original TFN, and adds encryption of communication between the attacker and stacheldraht masters and automated update of the agents.**	
February 8, 2000	Virii.tgz	A collection of files that are infected by a Linux/elf virus that could be out and spreading in the wild.	
February 8, 2000	Webscan.c	Multithreaded high speed scanner that records the versions of the web servers and scans for 65 different insecure CGIs.	
February 8, 2000	Wwwthreads.pl	Script that exploits the wwwthreads security vulnerability.	
February 7, 2000	Cgis.c	CGI scanner that works on Linux, OpenBSD, and others.	
February 7, 2000	CrackDate.zip	Cracks any Windows time limited program by changing the system date when the program is run/exits.	
February 7, 2000	Fw.c	FreeBSD kernel module that allows a certain IP to bypass ipfilter firewall rules.	
February 7, 2000	Utrojan.c	Universal remote UNIX Trojan, which can backdoor nearly any service on any platform.	
February 4, 2000	Config.h	A version of secfingerd's config.h file that tells secfingerd where to look for files and what messages to display.	
February 4, 2000	**Rpc.c**	**A small rpc scanner that currently checks for cmsd, ttdbserverd, sadmind, statd, and amd.**	
February 4, 2000	Ulogin.c	Universal login Trojan for any operating system.	
February 3, 2000	Bytesaber.c	Generates various TCP packets at your request.	
February 3, 2000	**Ex_tiny2.c**	**Script that exploits the Tiny FTPD vulnerability.**	
February 3, 2000	M000h.sh	A Denial of Service attack against Linux Telnet users on systems that use the /dev/pts terminals.	
February 2, 2000	Getdata.tar.gz	Sniffer made with libpcap that supports multiple protocols like TCP, UDP, ICMP, and IGMP.	
February 2, 2000	Instructor.c	S 32 bit instruction set auditor.	
February 2, 2000	RecyclerSnoper.exe	Script that exploits the Microsoft Recycle Bin Creation Vulnerability.	
February 2, 2000	Sara-2.1.6.tar.gz	A security analysis tool based on the SATAN model.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
February 2, 2000	warftpd-dos.c	Denial of Service exploit for the War-ftpd MKD/CWD commands vulnerability.	
February 1, 2000	**Outlook4.vuln.txt**	**Script which exploits the Outlook Express 5.02 vulnerability.**	
January 31, 2000	Apsend.tar.gx	A TCP/IP packet sender to test firewalls and other other network applications. It also includes a syn flood option and the land Denial of Service attack.	
January 31, 2000	Brutesh.sh	Brute-force Linux-PAM password cracker.	
January 31, 2000	Brutus-aet2.zip	Obtains usernames/passwords using a simple dictionary attack.	
January 31, 2000	Bypass.viruscheck.txt	Exploit code, which allows viruses and Trojans a safe haven on many Windows 95/98/NT systems.	
January 31, 2000	**Fw1_script.tag.txt**	**Code that exploits the Firewall-1 Strip Script Tags Vulnerability.**	
January 31, 2000	Hexit.c	Fake shellcode generator.	
January 31, 2000	**Iiscat.c**	**IIScat exploits the recent Microsoft Index Server vulnerability to read any file on the server.**	
January 31, 2000	Localscan.tar.gz	A perl-based front-end for nmap.	
January 31, 2000	mix.htm	Microimages X server for Windows allows anyone to kill your session and start a xterm on your machine.	
January 31, 2000	**PMTU.htm**	**A HP-UX 10.30/11.00 system can be used as an IP traffic amplifier. Small amounts of inbound traffic can result in larger amounts of outbound traffic, using ICMP MTU discovery packets.**	
January 31, 2000	Procfs4.htm	Exploit script for BSD local root procfs vulnerability.	
January 31, 2000	Sms.htm	SMS 2.0 Remote Control introduces a security risk that will allow a malicious user to run programs in system context.	
January 28, 2000	Linux-netbus-client-v0.4.tgz	NetBus client for Linux that works with NetBus 1.60.	
January 28, 2000	Nmap-2.3BETA14.tgz	A utility for network exploration or security auditing.	
January 28, 2000	Phide.tar.gz	A lkm that hides processes under Linux 2.0.	
January 28, 2000	**Qpop-exploit-net.c**	**A modified version of the original qpopper 3.0beta29 exploit.**	
January 28, 2000	Snuff-v0.7.1.tar.gz	A packet sniffer for Linux 2.0/2.2 that can monitor many streams at once.	
January 28, 2000	Sqlbf.zip	MsSQL server brute force tool.	
January 28, 2000	Taskigt.tar.gz	A lkm that gives root to a process.	
January 26, 2000	Saint-1.5.tar.gz	User-friendly network security scanner that runs on UNIX.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
January 26, 2000	Spank.c	Denial of Service attack that uses up lots of bandwidth.	
January 26, 2000	Xdestroy.c	Destroys all windows in an X display.	
January 25, 2000	ADMsxinmap.c	Solaris Solstice Internet Mail IMAP4 Server x86 exploit.	
January 25, 2000	Cis.zip	CIS vulnerability scanner that scans for remote vulnerabilities.	
January 25, 2000	Fw-bakd.htm	Placing Backdoors Through Firewalls version 1.5 that includes a backdoor for any kind of intrusion.	
January 25, 2000	Mi018en.htm	Shellcode programming for SCO.	
January 25, 2000	**Qpop-xploit.c**	**Remote Linux x86 exploit for Qpopper 3.0beta29 and below.**	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two-week period:

- **There has been an increase in intruders compromising systems by installing and using Distributed Denial of Service (DDoS) tools, such as Trin00, TFN, TFN2K, or Stacheldraht, for launching packet-flooding Denial of Service attacks. In some cases, intruders are exploiting known vulnerabilities to gain access to systems, which they then use to launch further attacks. More information regarding these type of attacks may be found at the CERT or NIPC web sites: http://www.cert.org and http://www.nipc.gov respectively.**
- A Denial of Service attack tool, stream.c, has been discovered which could cause Unix machines to stop responding. It floods the host with ACK's coming from random IPs with remote sequence numbers. This type of attack may be difficult to filter out as it may resemble "normal" traffic.
- A security threat has been discovered, cross-site scripting, which allows users to launch malicious programs on a victim's computer or capture information a person volunteers on a Web site. Unauthorized access may be gained to documentation, server services, and Internet servers. Domain based security policies may be violated and web form behavior can be altered.
- There has been an increase in systems being root compromised via the 'NXT' vulnerability in BIND.
- There has been an increase in probes on ports 1080, 1953, and 31337.
- Deployment of password stealing Trojans, attacking AOL users, has reportedly been on the rise.
- An increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333.

- Numerous systems are being root compromised via the sadmind (port 111) and BIND (port 53) vulnerabilities.
- The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.

Viruses

W95/WinExt (Windows 95 executable file worm): It is a memory-resident Windows e-mail aware worm. Every hour it checks for unread messages in the Outlook Inbox and replies to them with an infected attached file called TRYIT.EXE.

The virus has a choice of different phrases to use as the message text:

"Hi, See you soon"
"Salut. A+."
"A bientot"
"J'ai bien retu ton message, je m'en occupe rapidement. En
attendant, regardes le fichier joint.".

If the infected executable file is run, it installs itself by altering the WIN.INI file to automatically run \WINDOWS\SYSTEM\WINEXT.EXE each time Windows is started. The virus stores information in a file called WINEXT.DAT to avoid e-mailing the same person more than once. Between the 11th and 31st of July the virus will attempt to send a message to an e-mail address in France with an anniversary-related greeting.

W97/Db-A (Word 97 macro virus): A simple macro virus that seems to have originated in France. From the 6th to the end of both November and December in any year from 2000 onwards, the virus alters the Document Comments.

W97/Lupi-A (Word 97 macro virus): A virus, which attempts to overwrite infections of other viruses (Class infectors), by overwriting them with its own code. The virus code includes text that is not displayed:

Destroy Virus with Virus…

And

CISI-LUPI

WM97/Marker-AC (Word 97 macro virus): A variant of WM97/Marker, which drops files in the current directory. The files all have names of the type CMC*.txt where the * represents a number. The files contain the text "Railways is an integral part of CMC LTD. JAI CMC".

WM97/Melissa-AL (Word 97 macro virus and e-mail worm): This is a reworking of the original WM97/Melissa that has the same payloads.

W97M/SkyNet (Word 97 macro virus): A macro virus that infects Microsoft Word 97 documents as well as the global template. Whenever an infected document is opened, the virus infects the global template and will infect each of the documents used subsequently. Among its effects are the following:

- Impedes working with macros.
- Disables the antivirus security of Microsoft Word.

- Orders alphabetically by name all the Word documents in the directory by default whenever the year is later than 1999, the month is later than October, and the time is later than 20:00 hours.
- On the 18th of any month and year (later than 1999, from 8 p.m. onwards), it modifies the file that is executed on starting the computer (AUTOEXEC.BAT).

When an infected document is opened, the virus checks to see if the template is already infected. This is accomplished by searching for the text string "SkyNet" in the template. If it does not find it, it infects the template and subsequently infects all Word documents that are used by repeating the same operation in each one. The modification of the file that is executed on booting the computer (AUTOEXEC.BAT) causes the hard disk to be reformatted, and ALL its contents are lost.

WM97/Thursday-J (Word 97 macro virus): A variant of the WM97/Thursday Word macro virus. On November 3rd the virus creates a folder called C:\000_new containing a file called Thus_100.txt.
The file contains the text:

Testmakro Thus_100

WM97/Thursday-F (Word 97 macro virus): This virus is a variant of the WM97/Thursday Word macro virus.

XM97/Laroux-EG (Excel 97 macro virus): Another variant of XM/Laroux. It contains two macros, AUTO_OPEN and CHECK_FILES. The AUTO_OPEN macro is run when the infected document is opened, and instructs Excel to call the CHECK_FILES macro every time a new worksheet is activated.

When this happens, the virus creates a file in the XLSTART directory called PLDT.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run, much like Word's NORMAL.DOT. From then on, it infects every workbook used.

XM97/Laroux-MA (Excel 97 macro virus): Another variant of XM/Laroux. It contains two macros, AUTO_OPEN and VRS. The AUTO_OPEN macro is run when the infected document is opened, and instructs Excel to call the VRS macro every time a new worksheet is activated.

When this happens, the virus creates a file in the XLSTART directory called DIMON.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run, much like Word's NORMAL.DOT. From then on, it infects every workbook used.

VBS/Netlog.worm (VBScript worm): A new Internet-aware VBScript worm. A person does not have to manually run a VBScript file, or read an e-mail message to get infected; it spreads over open network shares.

The first thing it does is look for the file "c:\network.log". If it finds the file, it then deletes it and creates a new "c:\network.log" file and writes "Log file Open" to it. Next it writes the following to the "c:\network.log" file:

> “Subnet: [Random number between 199 and 214].[Random number between 1 and 254].[Random number between 1 and 254].0"

It then will start to scan the addresses. For instance, if it picked 10, 11, and 12, it would start scanning at 10.11.12.1, then 10.11.12.2, then 10.11.12.3, and so on, until it reached 10.11.12.255, and would randomly pick a new subnet to scan. After it has scanned 50 subnets in one run, it no longer limits the first part of the Internet address to numbers between 199 and 214, and can pick any address between 1 and 254.

When scanning, it uses Windows NetBIOS to look for open shares called "C". These are shared drives that users intended to share with their local network, but inadvertently shared over the entire Internet. It tries to map the remote drive as drive "J:"! If it succeeds it writes:

"Copying files to : [Network name of remote drive]"

to the "c:\network.log" file.

First as a test, it copies itself to the root directory of the remote drive and checks to see whether the copy was successful. If it was, it writes:

"Successful copy to : [Network name of remote drive]"

to the "c:\network.log" file. Then it will copy the network.vbs file to these directories:

```
"j:\windows\startm~1\programs\startup\"
"j:\windows\"
"j:\windows\start menu\programs\startup\"
"j:\win95\start menu\programs\startup\"
"j:\win95\startm~1\programs\startup\"
"j:\wind95\"
```

where J: is the remote drive C: the virus mapped earlier. This means that the worm gets control next time the victim starts their computer since J: actually means drive C:.

W95/Haiku.worm (worm): An Intranet aware worm, which travels via e-mail from the host system. It has the potential to overload network traffic, impacting the availability of resources. The increase in network traffic may degrade eBusiness performance, making end users unable to connect to e-mail and eCommerce sites.

The Haiku Worm arrives in an email with the subject line

``Fw: Compose your own haikus!"

The email will have the file Haiku.exe attached. The text of the message reads:

> "Old pond...
> a frog leaps in
> water's sound."
> -Matsuo Basho.
>
> DO YOU WANT TO COMPOSE YOUR OWN HAIKUS? Now you can! it is very easy to get started in this old poetry art. Attached to this e-mail you will find a copy of a simple haiku generator. It will help you in order to understand the basics of the metric, rhyme and subjects who should be used when composing a real haiku... just check it out! it's freeware and you can use and spread it as long as you want!

If Haiku.exe is run, it copies itself to C:\WINDOWS\HAIKUG.EXE and edits the WIN.INI file, so the Worm will be loaded when Windows is restarted. The Worm then displays a poem that is generated from an internal list of words. The program exits when the 'OK' button is selected.

The next time a computer is restarted, the Worm will be loaded automatically. At that point, it will not display any messages and is registered as a service, so that it doesn't appear in the tasklist.

The Worm stays resident, checking for an active dial-up Internet connection. When it finds one, it will search through files with the extension .doc, .eml, .htm, .html, .rtf and .txt looking for email addresses. The Haiku Worm then attempts to send a copy of itself to all of the email addresses that it has found.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

No new Trojan additions to this issue of CyberNotes.

Trojan	Version	Issue discussed
AOL Trojan		CyberNotes-2000-01
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
FakeFTP	Beta	CyberNotes-2000-02
Hack’A’tack	1.0-2000	CyberNotes-2000-01
InCommand	1.0-1.4	CyberNotes-2000-01
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01
Matrix	1.4-2.0	CyberNotes-2000-01
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02